HOMEWORK 9
DUE: 12/12

For reference, consult my notes, Davenport Chapter 6, or Niven and Zuckerman Chapter 5. For problems which partially or fully appear there or anywhere, please do not look at solutions; feel free to look at all other solved problems.

Suppose I have a set $S$, and a subset $R \subset S \times S$. Equivalently, I can repackage this information in the form of a “relation”: for $x, y \in S$ we say $x \sim y$—read $x$ is related to $y$—if $(x, y) \in R$. $\sim$ is called an equivalence relation if:

(a) For any $x \in S$, $x \sim x$.
(b) For any $x, y \in S$, $x \sim y \iff y \sim x$.
(c) For any $x, y, z \in S$, $x \sim y$ and $y \sim z \implies x \sim z$.

Given $x \in S$, the equivalence class of $x$, denoted $[x]$, is the set

$$[x] = \{ y \in S | x \sim y \}$$

Let $\mathcal{P}(S)$ be the power set of $S$, i.e. the set of subsets of $S$. We can define

$$S/\sim = \{ U \in \mathcal{P}(S) | U = [x] \text{ for some } x \in S \}$$

You should think of an equivalence relation as specifying a weaker version of equality on the set $S$, $[x]$ as the set of things weakly equivalent to $x$, and $S/\sim$ the set of elements of $S$ up to this weaker notion of equivalence. The best example we’ve dealt with thus far is the relation $\equiv \mod n$: $S = \mathbb{Z}$ with the relation $a \sim b$ if $a \equiv b \mod n$, for $x \in \mathbb{Z}$ $[x]$ is the congruence class of $x$, and $S/\sim$ is simply $\mathbb{Z}/n$.

**Problem 1.**

(a) Let $S$ be a set endowed with an equivalence relation $\sim$. Show that every $x \in S$ is contained in some equivalence class, and for $x, y \in S$, show that $[x] \cap [y] \neq \emptyset \iff [x] = [y]$. Thus the equivalence classes partition $S$.

(b) Recall we said that for two binary quadratic forms $q, Q$, $q$ is equivalent to $Q$, $q \sim Q$, if there is some substitution

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = \pm 1$ such that

$$Q(x', y') = q(x, y)$$

Show that this is equivalence relation on the set $S = Q(d)$ of binary quadratic forms of discriminant $d$.

(c) Recall that we say that $q$ and $Q$ are properly equivalent, $q \approx Q$, if $Q$ is obtained from $q$ by an invertible integral substitution as above but with $\det A = 1$. Show that this is also an equivalence relation on $Q(d)$.

**Problem 2.**

(a) Suppose $q(x, y) = ax^2 + bxy + cy^2$ is a quadratic form. Show that the discriminant $d(q) = b^2 - 4ac$ always satisfies $d(q) \equiv 0, 1 \mod 4$.

(b) Show that for any $d \in \mathbb{Z}$ with $d \equiv 0, 1 \mod 4$, there is a quadratic form with discriminant $d(q) = d$. 
Problem 3. Recall that a positive form \( q(x, y) = ax^2 + bxy + cy^2 \) is called properly reduced if either 
\(-a < b \leq a < c \) or \( 0 \leq b \leq a = c \).

(a) Show that if \( q(x, y) \) is properly reduced, then \( q'(x, y) = ax^2 + |b|xy + cy^2 \) is reduced and equivalent to \( q \).

(b) Show that there are finitely many properly reduced forms of a given discriminant.

(c) Show that every positive form is properly equivalent to a properly reduced form.

Problem 4. (N&Z Problem §5.14.2) Find the properly reduced form properly equivalent to each of the following positive binary quadratic forms, and the substitution inducing the equivalence:
(a) \( 3x^2 + 7xy + 5y^2 \);
(b) \( 2x^2 - 5xy + 4y^2 \);
(c) \( 2x^2 + xy + 6y^2 \);
(d) \( 3x^2 + xy + y^2 \).

Problem 5. Find all the reduced and properly reduced forms of discriminant:
(a) \(-12\);
(b) \(-19\);
(c) \(-23\);
(d) \(-39\).

Problem 6. Let \( Q(x, y) = Ax^2 + Bxy + Cy^2 \) be an indefinite binary quadratic form with positive discriminant. By echoing our proof for the case when \( Q \) is positive, show that \( Q \) is always properly equivalent to a form \( q(x, y) = ax^2 + bxy + y^2 \) with \(|b| \leq |a| \leq |c| \). Show by example that there are nonequal but properly equivalent forms satisfying \(|b| < |a| < |c| \). (Hint: Consider the integer \( a \) that is properly represented by \( Q \) and of minimal size \(|a|\).)